BINOMIAL RINGS: AXIOMATISATION, TRANSFER, AND CLASSIFICATION

Qimh Richey Xantcha[*]

16th January 2013

At the age of twenty-one he wrote a treatise upon the Binomial Theorem, which has had a European vogue.

— Sherlock Holmes's description of Professor Moriarty;
Arthur Conan Doyle, *The Final Problem*

Argument

A detailed study is made of *Binomial Rings*, rings with Binomial Co-efficients, as introduced by Hall. They are axiomatised and proved identical to the *Numerical Rings* studied by Ekedahl. A *Binomial Transfer Principle* is established, enabling combinatorial proofs of algebraical identities. The finitely generated Binomial Rings are completely classified, and like-wise the finitely generated, torsion-free modules.

2010 Mathematics Subject Classification. Primary: 13F99. Secondary: 13F20.

The ubiquity and utility of Binomial Co-efficients presumably require no detailed explanation. Their abstract study seems to have been initiated by Hall, [5], who introduced the concept of *Binomial Rings* in connexion with his ground-breaking work on nilpotent groups. The definition is simple: a Binomial Ring is a commutative, unital ring R which is torsion-free and closed in $\mathbf{Q}\otimes R$ under the "formation of binomial co-efficients":

$$r \mapsto \frac{r(r-1)\cdots(r-n+1)}{n!}.$$

Ekedahl, [2], preferring the axiomatic approach, proposed six axioms intended to capture the properties of Binomial Co-efficients. He appears not to have been familiar with the work of Hall and never proved the two *modi*

[*] Qimh Richey Xantcha, Uppsala University: qimh@math.uu.se

operandi to be equivalent. Rectifying this is one object of the present paper. Indeed, we not only justify, but improve upon Ekedahl's axioms, giving explicit formulæ (where none were given), as well as dropping the ghastliest axiom (the sixth):

Theorem 3. — *The following five axioms characterise the class of Binomial Rings:*

I. $$\binom{a+b}{n} = \sum_{p+q=n} \binom{a}{p}\binom{b}{q}.$$

II. $$\binom{ab}{n} = \sum_{m=0}^{n} \binom{a}{m} \sum_{\substack{q_1+\cdots+q_m=n \\ q_i \geqslant 1}} \binom{b}{q_1} \cdots \binom{b}{q_m}.$$

III. $$\binom{a}{m}\binom{a}{n} = \sum_{k=0}^{n} \binom{a}{m+k}\binom{m+k}{n}\binom{n}{k}.$$

IV. $$\binom{1}{n} = 0 \quad \textit{when } n \geqslant 2.$$

V. $$\binom{a}{0} = 1 \quad \textit{and} \quad \binom{a}{1} = a.$$

The missing sixth axiom will be duly commented upon.

What is known on Binomial Rings stems principally from rather a recent paper [3] by Elliott, which in particular aims to elucidate the connexion between binomial rings and λ-rings. Let us compile a list of their most important properties.

1. The Free Binomial Ring on the set X is the ring

$$\{f \in \mathbf{Q}[X] \mid f(\mathbf{Z}^X) \subseteq \mathbf{Z}\}.$$

of integer-valued polynomials on X. ([3], Proposition 2.1.)

2. The following conditions on a commutative, unital ring R are equivalent ([3], Theorem 4.1, 4.2):

   A. R is the quotient of a binomial ring.

   B. The elements of R satisfy every integer *polynomial congruence* universally true for the integers.

   C. $a(a-1)\cdots(a-n+1)$ is divisible by $n!$ for every $n \in \mathbf{N}$.

   D. *Fermat's Little Theorem* holds: $a^p \equiv a \bmod pR$ for every prime p.

   E. The Frobenius map $a \mapsto a^p$ is the identity on R/pR for every prime p.

F. R/pR is reduced for every prime p, and the residue field of R/pR is isomorphic to $\mathbf{Z}/p$.

These transform into criteria for binomial rings if, in each case, an assumption on lack of torsion be added.

3. The binomial property is preserved under the following constructions: localisation, direct and tensor products, filtered inductive and projective limits. ([3], Propositions 5.1, 5.4, 5.5.)
4. The inclusion functor from Binomial Rings to Rings has both a left and a right adjoint. ([3], Theorems 7.1, 9.1.)
5. Binomial rings are equivalent to λ-rings with trivial Adams operations. ([7] Proposition 1.2, [3] Proposition 8.3.)
6. *The Binomial Theorem*: Let R be binomial and let A be a commutative algebra over R which is complete with respect to the ideal I. The equation

$$(1+x)^r = \sum_{n=0}^{\infty} \binom{r}{n} x^n$$

defines an R-module structure on the abelian group $(1+I, \cdot)$. ([3], Proposition 11.1.)

As a contribution to the theory, we prove the following *Transfer Principle*, formally sanctioning combinatorial proofs of algebraical identities in binomial rings. It may be favourably compared to property 2B above.

Theorem 6: The Binomial Transfer Principle. — *A binomial polynomial identity universally valid in* $\mathbf{Z}$ *is valid in every binomial ring.*

We also prove the following Classification Theorem.

Theorem 10: The Structure Theorem for Finitely Generated Binomial Rings. — *Let R be a finitely generated binomial ring. There exist unique positive, simply composite integers $m_1, \dots, m_k$ such that*

$$R \cong \mathbf{Z}[m_1^{-1}] \times \cdots \times \mathbf{Z}[m_k^{-1}].$$

Binomial rings naturally manifest themselves in the theories of integer-valued polynomials, Witt vectors, and λ-rings; to name but a few. We refer the reader to Elliott's article [3] and the lucid monograph [11] by Yau, where these topics have been expounded upon.

More recently, binomial rings have turned out to form the natural framework for discussing polynomial maps and functors of modules; see [8], [9], and [10].

§1. Definitions and Examples

Let us first state Hall's original definition, as found in [5].

Definition 1 ([5], Section 6). — Let R be a commutative ring with unity. It is a **binomial ring** if it is torsion-free[1] and closed in $\mathbf{Q} \otimes R$ under the operations

$$r \mapsto \frac{r(r-1)\cdots(r-n+1)}{n!}.$$

We next present, with minor modifications, Ekedahl's axioms for numerical rings, with the notable exception of the sixth. The original axioms in [2] were rather non-explicit, stated, as they were, in terms of the same three mysterious polynomials occurring in the theory of λ-rings. Our definition intends to remedy this.

Definition 2 ([2], Definition 4.1). — A **numerical ring** is a commutative ring with unity equipped with unary operations

$$r \mapsto \binom{r}{n}, \quad n \in \mathbf{N};$$

called **binomial co-efficients** and subject to the following axioms:

I. $\displaystyle \binom{a+b}{n} = \sum_{p+q=n} \binom{a}{p}\binom{b}{q}.$

II. $\displaystyle \binom{ab}{n} = \sum_{m=0}^{n} \binom{a}{m} \sum_{\substack{q_1+\cdots+q_m=n \\ q_i \geqslant 1}} \binom{b}{q_1} \cdots \binom{b}{q_m}.$

III. $\displaystyle \binom{a}{m}\binom{a}{n} = \sum_{k=0}^{n} \binom{a}{m+k}\binom{m+k}{n}\binom{n}{k}.$

IV. $\displaystyle \binom{1}{n} = 0 \quad \text{when } n \geqslant 2.$

V. $\displaystyle \binom{a}{0} = 1 \quad \text{and} \quad \binom{a}{1} = a.$

Conspicuously absent is a formula for reducing a *composition* $\binom{\binom{a}{m}}{n}$ of binomial co-efficients to simple ones, included as Ekedahl's sixth axiom. Surprisingly, such a formula will turn out to be a consequence of the five axioms listed.

[1] The word *torsion* will, here and elsewhere, be taken to mean $\mathbf{Z}$*-torsion*.

It follows easily from Axioms I, IV, and V that, when the functions $\binom{-}{n}$ are evaluated on multiples of unity, we retrieve the ordinary binomial co-efficients, namely

$$\binom{m\cdot 1}{n} = \frac{m(m-1)\cdots(m-n+1)}{n!}\cdot 1, \quad m\in\mathbf{N}.$$

Since $\binom{n\cdot 1}{n} = 1$, but $\binom{0}{n} = 0$ unless $n = 0$, a numerical ring has necessarily characteristic 0.

Our present objective will be shewing that numerical and binomial rings co-incide. It follows that the numerical structure on a given ring is always unique.

Example 1. — In any $\mathbf{Q}$-algebra, binomial co-efficients may be defined by the usual formula:

$$\binom{r}{n} = \frac{r(r-1)\cdots(r-n+1)}{n!}.$$

△

Example 2. — For any integer m, the ring $\mathbf{Z}[m^{-1}]$ is numerical. Since it inherits the binomial co-efficients from $\mathbf{Q}$, it is simply a question of verifying closure under the formation of binomial co-efficients. Because

$$\binom{\frac{a}{f}}{n} = \frac{\frac{a}{f}(\frac{a}{f}-1)\cdots(\frac{a}{f}-(n-1))}{n!} = \frac{a(a-f)\cdots(a-(n-1)f)}{n!f^n},$$

it will suffice to prove that whenever $p^i \mid n!$, but $p\nmid b$, then

$$p^i \mid (a+b)(a+2b)\cdots(a+nb).$$

To this end, let

$$n = c_m p^m + \cdots + c_1 p + c_0, \qquad 0\leqslant c_i \leqslant p-1,$$

be the base p representation of n. For fixed k and $0\leqslant d < c_k$, the numbers

$$a + (c_m p^m + \cdots + c_{k+1}p^{k+1} + dp^k + i)b, \qquad 1\leqslant i\leqslant p^k, \tag{1}$$

will form a set of representatives for the congruence classes modulo p^k, as will of course the numbers

$$c_m p^m + \cdots + c_{k+1}p^{k+1} + dp^k + i, \qquad 1\leqslant i\leqslant p^k. \tag{2}$$

Note that if $x\equiv y \bmod p^k$ and $j\leqslant k$, then $p^j \mid x$ iff $p^j\mid y$. Hence there are at least as many factors p among the numbers (1) as among the numbers (2). The claim now follows. △

EXAMPLE 3. — As the special case $m = 1$ of the preceding example, $\mathbf{Z}$ itself is numerical. For this ring there is another, more direct, way of proving the numerical axioms. Let us indicate how they may be arrived at as solutions to problems of Enumerative Combinatorics.

> *Axiom I.* We have two types of balls: round balls, square[2] balls. If we have a round balls and b square balls, in how many ways may we choose n balls? Let p be the number of round balls chosen, and q the number of square balls.
>
> *Axiom II.* We have a chocolate box containing a rectangular $a \times b$ array of pralines, and we wish to eat n of these. In how many ways can this be done? Suppose the pralines we choose to feast upon are located in m of the a rows, and let q_i be the number of chosen pralines in row number i of these m.
>
> *Axiom III.* There are a Mathematicians, of which m do Geometry and n Algebra. Naturally, there may exist people who do both or neither. How many distributions of skills are possible? Let k be the number of Mathematicians who do only Algebra.
>
> *Axiom IV.* We are the owner of a single dog. In how many ways can we choose n of our dogs to take for a walk?
>
> *Axiom V.* Snuffy the dog has a blankets. In how many ways may he choose 0 (in the summer) or 1 (in the winter) of his blankets to keep him warm in bed?

△

EXAMPLE 4. — Being given by rational polynomials, the operations $r \mapsto \binom{r}{n}$ give continuous maps $\mathbf{Q}_p \to \mathbf{Q}_p$ in the p-adic topology. It should be well known that $\mathbf{Z}$ is dense in the ring $\mathbf{Z}_p$, and that $\mathbf{Z}_p$ is closed in $\mathbf{Q}_p$. Since the binomial co-efficients leave $\mathbf{Z}$ invariant, the same must be true of $\mathbf{Z}_p$, which is thus numerical.

This provides an alternative proof of the fact that $\mathbf{Z}[m^{-1}]$ is closed under binomial co-efficients. For this is evidently true of the localisations

$$\mathbf{Z}_{(p)} = \mathbf{Q} \cap \mathbf{Z}_p,$$

and therefore also for

$$\mathbf{Z}[m^{-1}] = \bigcap_{p \nmid m} \mathbf{Z}_{(p)}.$$

△

[2] This is in honour of Dr Lars-Christer Böiers of Lund, an eminent teacher, who gave an example featuring round balls and square balls during his course in Discrete Mathematics.

§2. Elementary Identities

Theorem 1. — *The following formulæ are valid in any numerical ring:*

1. $\displaystyle\binom{r}{n} = \frac{r(r-1)\cdots(r-n+1)}{n!}$ *when* $r \in \mathbf{Z}$.
2. $\displaystyle n!\binom{r}{n} = r(r-1)\cdots(r-n+1)$.
3. $\displaystyle n\binom{r}{n} = (r-n+1)\binom{r}{n-1}$.

Proof. The map

$$\varphi\colon (R,+) \to (1+tR[[t]],\cdot), \qquad r \mapsto \sum_{n=0}^{\infty}\binom{r}{n}t^n$$

is, by Axioms I and V, a group homomorphism. Therefore, when $r \in \mathbf{Z}$,

$$\varphi(r) = \varphi(1)^r = (1+t)^r,$$

which expands as usual (with ordinary binomial co-efficients) by the Binomial Theorem. This proves Equation 1. (An inductive proof will also work.)

To prove Equations 2 and 3, we proceed differently. By Axiom III,

$$\begin{aligned} r\binom{r}{n-1} &= \binom{r}{n-1}\binom{r}{1} = \sum_{k=0}^{1}\binom{r}{n-1+k}\binom{n-1+k}{1}\binom{1}{k} \\ &= \binom{r}{n-1}\binom{n-1}{1}\binom{1}{0} + \binom{r}{n}\binom{n}{1}\binom{1}{1} \\ &= (n-1)\binom{r}{n-1} + n\binom{r}{n}, \end{aligned}$$

which reduces to Equation 3.

Equation 2 will then follow inductively from Equation 3. □

§3. Numerical versus Binomial Rings

The crucial step towards shewing the equivalence of binomial and numerical rings is demonstrating the lack of torsion in the latter class.

Lemma 1. — *Let m be an integer. If p is prime and $p^l \mid m$, but $p \nmid k$, then $p^l \mid \binom{m}{k}$.*

Proof. p^l divides the right-hand side of

$$k\binom{m}{k} = m\binom{m-1}{k-1},$$

and therefore also the left-hand side. But p^l is relatively prime to k, so in fact $p^l \mid \binom{m}{k}$. □

Lemma 2. — *Let $m_1, \dots, m_k$ be natural numbers, and put*

$$m = m_1 + \cdots + m_k.$$

If

$$n = m_1 + 2m_2 + 3m_3 + \cdots + km_k$$

is prime, then

$$m \mid \binom{m}{\{m_i\}},$$

unless $m_1 = m = n$, and all other $m_i = 0$.

Proof. Let a prime power $p^l \mid m$. Because of the relation $n = \sum m_i i$, then, save for the exceptional case

$$m_1 = m = p = n$$

given above, not all m_i can be divisible by p. Say $p \nmid m_j$; then

$$\binom{m}{\{m_i\}_i} = \binom{m}{m_j}\binom{m - m_j}{\{m_i\}_{i \neq j}}$$

is divisible by p^l according to Lemma 1. The claim follows. □

Lemma 3. — *Consider a numerical ring R. Let $r \in R$ and $m, n \in \mathbf{N}$. If $nr = 0$, then also $mn\binom{r}{m} = 0$.*

Proof. Follows inductively, since if $nr = 0$, then

$$mn\binom{r}{m} = n(r - m + 1)\binom{r}{m-1} = -n(m-1)\binom{r}{m-1}.$$

□

Theorem 2. — *Numerical rings are torsion-free.*

Proof. Suppose $nr = 0$ in R, and, without any loss of generality, that n is prime. We calculate using the numerical axioms:

$$\begin{aligned} 0 = \binom{0}{n} = \binom{nr}{n} &= \sum_{m=0}^{n} \binom{r}{m} \sum_{\substack{q_1 + \cdots + q_m = n \\ q_i \geqslant 1}} \binom{n}{q_1} \cdots \binom{n}{q_m} \\ &= \sum_{m=0}^{n} \binom{r}{m} \sum_{\substack{\sum m_i = m \\ \sum m_i i = n}} \binom{m}{\{m_i\}} \prod_i \binom{n}{i}^{m_i}. \end{aligned}$$

For given numbers q_i, we have let m_i denote the number of these that are equal to i (of course $i \geqslant 1$ and $m_i \geqslant 0$). Conversely, when the numbers m_i are given, values may be distributed to the numbers q_i in $\binom{m}{\{m_i\}}$ ways, which accounts for the multinomial co-efficient above.

We claim the inner sum is divisible by mn when $m \geqslant 2$. Indeed, when $2 \leqslant m \leqslant n-1$, then $m \mid \binom{m}{\{m_i\}}$ by Lemma 2. Also, there must exist some $0 < j < n$ such that $m_j > 0$, and for this j, Lemma 1 asserts $n \mid \binom{n}{j}^{m_j}$. In the case $m = n$, obviously all $m_i = 0$ for $i \geqslant 2$, and $m_1 = n$, and the inner sum will equal $\binom{n}{1}^n$, which is divisible by $n^2 = mn$.

We can now employ Lemma 3 to kill all terms except $m = 1$. But this term is simply $\binom{r}{1} = r$, which is then equal to 0. □

Theorem 3. — *Numerical and Binomial Rings co-incide.*

Proof. Clearly, binomial rings satisfy the numerical axioms.

Conversely, numerical rings are torsion-free, and their binomial co-efficients fulfil

$$n!\binom{r}{n} = r(r-1)\cdots(r-n+1)$$

by Theorem 1, and hence

$$\binom{r}{n} = \frac{r(r-1)\cdots(r-n+1)}{n!}.$$

□

The appellations *numerical* and *binomial* may thus be treated synonymously.

Let us now resolve the mystery of the missing sixth axiom. In $\mathbf{Z}$, there "exists" a formula for iterated binomial co-efficients:

$$\binom{\binom{r}{m}}{n} = \sum_{k=1}^{mn} g_k \binom{r}{k}, \tag{3}$$

in the sense that there are unique integers g_k making the formula valid for every $r \in \mathbf{Z}$. Golomb has examined these iterates in some detail, and his paper [4] is brought to an end with the discouraging conclusion:

> No simple reduction formulas have yet been found for the most general case of $\binom{\binom{n}{b}}{a}$.

Note, however, that (3) is a polynomial identity with rational co-efficients, by which it must hold in every $\mathbf{Q}$-algebra, and therefore in every binomial ring. This proves the redundancy of Ekedahl's original sixth axiom:

Theorem 4. — *The formula*

$$\binom{\binom{r}{m}}{n} = \sum_{k=1}^{mn} g_k \binom{r}{k}$$

for iterated binomial co-efficients is valid in every binomial ring.

§4. Binomial Transfer

Let X be a set, and let $E(X)$ be the *term algebra*[3] based on X. It consists of all finite words that can be formed from the alphabet

$$X \cup \left\{ +, -, \cdot, 0, 1, \binom{-}{n} \,\middle|\, n \in \mathbf{N} \right\},$$

where the symbols $+$ and $\cdot$ are binary, $-$ and $\binom{-}{n}$ are unary, and 0 and 1 nullary (constants).

Definition 3. — The ring $\mathbf{Z}\binom{X}{-}$ is the result of imposing upon the term algebra the axioms of a commutative ring with unity, as well as the Numerical Axioms.

Theorem 5. — *There is an isomorphism*

$$\mathbf{Z}\binom{X}{-} \cong \{f \in \mathbf{Q}[X] \mid f(\mathbf{Z}^X) \subseteq \mathbf{Z}\},$$

which is thus the free binomial ring on the set X. (Confer property 1 in the introductory section.)

Proof. The Numerical Axioms, together with the formula for iterated binomial co-efficients, will reduce any element of $\mathbf{Z}\binom{X}{-}$ to a binomial polynomial. Conversely, it is well known that any integer-valued polynomial is given by a binomial polynomial. □

Theorem 6: The Binomial Transfer Principle. — *A binomial polynomial identity universally valid in* $\mathbf{Z}$ *is valid in every binomial ring.*

Proof. Suppose $p(x_1, \dots, x_k) = 0$ is valid for any integer values of $x_1, \dots, x_k$. By the previous theorem, there is a canonical embedding

$$\mathbf{Z}\binom{x_1, \dots, x_k}{-} \to \mathbf{Z}^{\mathbf{Z}^k}$$
$$p(x_1, \dots, x_k) \mapsto (p(n_1, \dots, n_k))_{(n_1, \dots, n_k) \in \mathbf{Z}^k}.$$

View p as an element of $\mathbf{Z}\binom{x_1, \dots, x_k}{-}$. It is the zero binomial map, and therefore also the zero binomial polynomial. □

§5. Binomial Ideals and Factor Rings

Let us now make a short survey of binomial ideals and the associated factor rings.

[3] The denomination *term algebra* is borrowed from Universal Algebra; confer Definition II.10.4 of [1].

Theorem 7. — *Let I be an ideal of the binomial ring R. The equation*

$$\binom{r+I}{n} = \binom{r}{n} + I$$

will yield a binomial structure on R/I if and only if

$$\binom{e}{n} \in I$$

for every $e \in I$ and $n > 0$.

Proof. The condition is clearly necessary. To shew sufficiency, note that, when $r \in R$, $e \in I$, and the condition is satisfied, then

$$\binom{r+e}{n} = \sum_{p+q=n} \binom{r}{p}\binom{e}{q} \equiv \binom{r}{n}\binom{e}{0} = \binom{r}{n} \bmod I.$$

The Numerical Axioms in R/I follow immediately from those in R. □

Definition 4. — An ideal of a binomial ring satisfying the condition of the previous theorem will be called a **binomial ideal**.

Example 5. — $\mathbf{Z}$ does not possess any non-trivial binomial ideals, because all its non-trivial factor rings have torsion. Neither do the rings $\mathbf{Z}[m^{-1}]$. △

The next theorem provides a kind of converse.

Theorem 8. — *Let R be a (commutative, unital) ring, and let I be an ideal. Suppose I is a vector space over $\mathbf{Q}$, and that R/I is binomial. Then R itself is binomial, and I is a binomial ideal.*

Proof. Since I and R/I are both torsion-free, so is R, and there is a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, equal] & R \arrow[r] \arrow[d] & R/I \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q} \otimes_{\mathbf{Z}} I \arrow[r] & \mathbf{Q} \otimes_{\mathbf{Z}} R \arrow[r] & \mathbf{Q} \otimes_{\mathbf{Z}} R/I \arrow[r] & 0
\end{tikzcd}$$

It will suffice to shew that R is closed under the formation of binomial coefficients in $\mathbf{Q} \otimes R$. Let $r \in R$. Calculating in in the ring $\mathbf{Q} \otimes R/I$ yields

$$\frac{r(r-1)\cdots(r-n+1)}{n!} + I = \binom{r+I}{n}.$$

Since $\binom{r+I}{n}$ in fact lies in R/I, it must be that

$$\frac{r(r-1)\cdots(r-n+1)}{n!} \in R,$$

and we are finished.

That I is binomial follows from the fact that it is a vector space over $\mathbf{Q}$. □

§6. Finitely Generated Binomial Rings

Lemma 4. — *If a ring R is torsion-free and finitely generated as an abelian group, its fraction ring is $\mathbf{Q} \otimes R$.*

Proof. By the Structure Theorem for Finitely Generated Abelian Groups, R is isomorphic to some $\mathbf{Z}^n$ as an abelian group. Let $a \in \mathbf{Z}^n$. Multiplication by a is a linear transformation on $\mathbf{Z}^n$, and so may be represented by an integer matrix A. The condition that a not be a zero-divisor corresponds to A being non-singular. It will then have an inverse A^{-1} with *rational* entries. The inverse of a is given by

$$a^{-1} = A^{-1}1 \in \mathbf{Q}^n = \mathbf{Q} \otimes R,$$

where 1 denotes the multiplicative identity of R, considered as a column vector. □

Lemma 5. — *Let A denote the algebraic integers in the field $K \supseteq \mathbf{Q}$. If K is finitely generated over $\mathbf{Q}$, then A is finitely generated over $\mathbf{Z}$.*

The subsequent (in)equality of Krull dimensions is supposedly familiar to scholars in the fields of Commutative Algebra or Algebraic Geometry. We are grateful to Professor Ekedahl for furnishing the proof.

Theorem 9: Chevalley's Dimension Argument. — *Let R be a finitely generated, non-trivial, commutative, unital ring. The (in)equality*

$$\dim R/pR = \dim \mathbf{Q} \otimes_{\mathbf{Z}} R \leqslant \dim R - 1$$

holds for all but finitely many prime numbers p.

When R is an integral domain of characteristic 0, there is in fact equality for all but finitely many primes p.

Proof. In the case of positive characteristic n, the inequality will hold trivially, for then

$$\mathbf{Q} \otimes_{\mathbf{Z}} R = 0 = R/pR,$$

except when $p \mid n$.

Consider now the case when R is an integral domain of characteristic 0. There is an embedding $\varphi\colon \mathbf{Z} \to R$, and a corresponding dominant morphism

$$\operatorname{Spec}\varphi\colon \operatorname{Spec} R \to \operatorname{Spec} \mathbf{Z}$$

of integral schemes, which is of finite type. Letting $\operatorname{Frac} P$ denote the fraction field of R/P, we may define

$$\begin{aligned} C_n &= \{P \in \operatorname{Spec}\mathbf{Z} \mid \dim(\operatorname{Spec}\varphi)^{-1}(P) = n\} \\ &= \{P \in \operatorname{Spec}\mathbf{Z} \mid \dim R \otimes \operatorname{Frac} P = n\} \\ &= \{(p) \mid \dim R/pR = n\} \cup \{(0) \mid \dim R \otimes \mathbf{Q} = n\}. \end{aligned}$$

This latter set, by Chevalley's Constructibility Theorem[4], will contain a dense, open set in $\operatorname{Spec}\mathbf{Z}$ if $n = \dim R - \dim \mathbf{Z}$. Such a set must contain (0) and (p) for all but finitely many primes p, so for those primes,

$$\dim \mathbf{Q} \otimes_{\mathbf{Z}} R = \dim R/pR = \dim R - 1.$$

Now let R be an arbitrary ring of characteristic 0. For any prime ideal Q, R/Q will be an integral domain (but not necessarily of characteristic 0), and so we can apply the preceding to obtain

$$\dim \mathbf{Q} \otimes_{\mathbf{Z}} R/Q = \dim R/(Q+pR) \leqslant \dim R/Q - 1,$$

for all but finitely many primes p. The prime ideals of $\mathbf{Q} \otimes_{\mathbf{Z}} R$ are of the form $\mathbf{Q} \otimes_{\mathbf{Z}} Q$, where Q is a prime ideal in R. Moreover,

$$(\mathbf{Q} \otimes_{\mathbf{Z}} R)/(\mathbf{Q} \otimes_{\mathbf{Z}} Q) = \mathbf{Q} \otimes_{\mathbf{Z}} R/Q.$$

It follows that

$$\begin{aligned} \dim \mathbf{Q} \otimes_{\mathbf{Z}} R &= \max_{Q \in \operatorname{Spec} R} \dim (\mathbf{Q} \otimes_{\mathbf{Z}} R)/(\mathbf{Q} \otimes_{\mathbf{Z}} Q) \\ &= \max_{Q \in \operatorname{Spec} R} \dim \mathbf{Q} \otimes_{\mathbf{Z}} R/Q \\ &= \max_{Q \in \operatorname{Spec} R} \dim R/(Q+pR) \\ &= \max_{\overline{Q} \in \operatorname{Spec} R/pR} (R/pR)/\overline{Q} = \dim R/pR \end{aligned}$$

for all but finitely many p, because the maxima are taken over the finitely many *minimal* prime ideals only. In a similar fashion,

$$\begin{aligned} \dim \mathbf{Q} \otimes_{\mathbf{Z}} R &= \max_{Q \in \operatorname{Spec} R} \dim (\mathbf{Q} \otimes_{\mathbf{Z}} R)/(\mathbf{Q} \otimes_{\mathbf{Z}} Q) \\ &= \max_{Q \in \operatorname{Spec} R} \dim \mathbf{Q} \otimes_{\mathbf{Z}} R/Q \\ &\leqslant \max_{Q \in \operatorname{Spec} R} \dim R/Q - 1 \leqslant \dim R - 1. \end{aligned}$$

□

The following Classification Theorem, together with its proof, was communicated to us by Professor Ekedahl.

Theorem 10: The Structure Theorem for Finitely Generated Binomial Rings. — *Let R be a finitely generated binomial ring. There exist unique positive, simply composite[5] integers $m_1, \dots, m_k$ such that*

$$R \cong \mathbf{Z}[m_1^{-1}] \times \cdots \times \mathbf{Z}[m_k^{-1}].$$

[4] This proposition appears to belong to the folklore of Algebraic Geometry. An explicit reference is Théorème 2.3 of [6].

[5] A *simply composite*, or *square-free*, number is a positive integer that is a (possibly empty) product of distinct primes.

Proof. Case A: R is finitely generated as an abelian group. We impose the stronger hypothesis that R be finitely generated as an abelian group.

If $r^n = 0$, then, because of Fermat's Little Theorem (property 2 in the introduction), r is divisible by p for all primes $p > n$. But in $\mathbf{Z}^n$ this can only be if $r = 0$; hence R is reduced. By the lemma above, the fraction ring of R is $\mathbf{Q} \otimes R$. As this is reduced and artinian, being finite-dimensional over $\mathbf{Q}$, it splits up into a product of fields of characteristic 0.

Case A1: The fraction ring of R is a field. Let us first consider the special case when the fraction ring $\mathbf{Q} \otimes R$ is a field, whose ring of algebraic integers we denote by A. We examine the subgroup $A \cap R$ of A. Since $A \subseteq \mathbf{Q} \otimes R$, an arbitrary element of A will have an integer multiple lying in R. This means $A/(A \cap R)$ is a torsion group. Also, the fraction ring $\mathbf{Q}\otimes R$ is finitely generated over $\mathbf{Q}$, so, from the lemma above, we deduce that A is finitely generated over $\mathbf{Z}$. Because the factor group $A/(A \cap R)$ is both finitely generated and torsion, it is killed by a single integer N, so that

$$N(A/(A \cap R)) = 0,$$

and, as a consequence,

$$(A \cap R)[N^{-1}] = A[N^{-1}].$$

Now let $z \in A$ and let p be a prime. The element

$$z \in A[N^{-1}] = (A \cap R)[N^{-1}]$$

can be written $z = \frac{a}{N^k}$, where $a \in A \cap R$ and $k \in \mathbf{N}$. Using Fermat's Little Theorem, we find that

$$(N^k)^p = N^k + pn$$
$$a^p = a + pb$$

for some $n \in \mathbf{Z}$ and $b \in R$. Observe that pb belongs to $A \cap R$, hence to $A[N^{-1}]$, so that $b \in A$, as long as p does not divide N. We then have

$$\begin{aligned} z^p - z &= \frac{a^p}{N^{kp}} - \frac{a}{N^k} = \frac{a+pb}{N^k+pn} - \frac{a}{N^k} \\ &= \frac{(a+pb)N^k - a(N^k+pn)}{(N^k+pn)N^k} = p\frac{N^k b - na}{(N^k+pn)N^k} = p\frac{N^k b - na}{N^{(p+1)k}}, \end{aligned}$$

and hence

$$pu = z^p - z \in A$$

for some $u \in A[N^{-1}]$, assuming $p \nmid N$. But then in fact $u \in A$.

Consequently, for all $z \in A$ and all sufficiently large primes p, the relation $z^p - z \in pA$ holds, so that $z^p = z$ in A/pA. Being reduced and artinian, A/pA may be written as a product of fields, and, because of the equation $z^p = z$, these fields must all equal $\mathbf{Z}/p$, which means all sufficiently large primes split completely in A. It will then be a consequence of Chebotarev's Density Theorem[6] that $\mathbf{Q} \otimes R = \mathbf{Q}$. Since we are working under the assumption that R is finitely generated as an abelian group, we infer that $R = \mathbf{Z}$.

Case A2: The fraction ring of R is a product of fields. If the fraction ring of R is a product $\prod K_j$ of fields, the projections R_j of R on the factors K_j will each be binomial. Hence $R \subseteq \prod R_j$, with each R_j being isomorphic to $\mathbf{Z}$, according to the above argument. But $\mathbf{Z}$ possesses no non-trivial binomial ideals, so by Goursat's Lemma, R must equal the whole product

$$R = \prod R_j = \prod \mathbf{Z}.$$

Case B: R is not finitely generated as an abelian group. Finally, we drop the assumption that R be finitely generated as a group, and assume it finitely generated as a ring only. Because of the relation $p \mid r^p - r$, R/pR will be a finitely generated torsion group for each prime p. It will then have Krull dimension 0, and it follows from Chevalley's Dimension Argument that $\dim \mathbf{Q} \otimes R = 0$, so that $\mathbf{Q} \otimes R$ is a finite-dimensional vector space over $\mathbf{Q}$. Only finitely many denominators can be employed in a basis, so there exists an integer M for which $R[M^{-1}]$ is finitely generated over $\mathbf{Z}[M^{-1}]$.

We can now more or less repeat the previous argument. $R[M^{-1}]$ will still be reduced, and as before, $\mathbf{Q} \otimes R[M^{-1}]$ will be finite-dimensional, hence a product of fields, and we may reduce to the case when $\mathbf{Q} \otimes R[M^{-1}]$ is a field. Letting A denote the algebraic integers in $\mathbf{Q} \otimes R[M^{-1}]$, the factor group $A/R[M^{-1}]$ will be finitely generated and torsion, and hence killed by some integer, so that again we are lead to $R[N^{-1}] = A[N^{-1}]$. As before, we may draw the conclusion that $\mathbf{Q} \otimes R = \mathbf{Q}$, and consequently that $R = \mathbf{Z}[N^{-1}]$. This concludes the proof of existence.

Uniqueness. Note that

$$S = \mathbf{Z}[m_1^{-1}] \times \cdots \times \mathbf{Z}[m_k^{-1}]$$

is characterised, among rings of this same type, by the following properties:

1. There exist k elements $e_1, \ldots, e_k \in S$ such that:
   (a) The set $\{e_1, \ldots, e_k\}$ is a basis for $\mathbf{Q} \otimes S$.
   (b) $e_i e_j = \delta_{ij} e_i$ (Kronecker delta).
2. Any such basis may be renumbered $\{e_1, \ldots, e_k\}$ so that e_j be divisible by a simply composite n_j (in S) if and only if $n_j \mid m_j$.

The first property shews that the number k is uniquely determined, and the second that different values for m_i yield non-isomorphic rings. □

[6] (A special case of) Chebotarev's Density Theorem states the following: The density of the primes that split completely in a number field K equals $\frac{1}{|\mathrm{Gal}(K/\mathbf{Q})|}$. In our case, this set has density 1.

§7. Torsion-Free Modules

An elegant application of the Structure Theorem is the classification of torsion-free modules.

Lemma 6. — *Consider a ring homomorphism* $\varphi\colon R \to S$. *If* R *is binomial and* S *is torsion-free, then* $\operatorname{Ker}\varphi$ *will be a binomial ideal.*

Proof. If $r \in \operatorname{Ker}\varphi$ and $n > 0$, then

$$n!\varphi\left(\binom{r}{n}\right) = \varphi\left(n!\binom{r}{n}\right) = \varphi(r(r-1)\cdots(r-n+1)) = 0.$$

Thus $\binom{r}{n} \in \operatorname{Ker}\varphi$. □

Let M be a torsion-free module over the binomial ring R, with module structure given by the group homomorphism

$$\mu\colon R \to \operatorname{End} M.$$

We have the following commutative diagram:

$$\begin{tikzcd}
 & & & & 0 \arrow[dl] \\
0 \arrow[r] & \operatorname{Ker}\mu \arrow[r] & R \arrow[r] \arrow[d, "\mu"'] & R/\operatorname{Ker}\mu \arrow[r] \arrow[dl] & 0 \\
 & & \operatorname{End} M & &
\end{tikzcd}$$

The group $\operatorname{End} M$ is torsion-free, so, by the lemma, $\operatorname{Ker}\mu$ is a binomial ideal. Therefore M will in fact be a module over the binomial ring $R/\operatorname{Ker}\mu$.

Let us now also assume that $\operatorname{End} M$ is finitely generated (as a module) over $\mathbf{Z}[n^{-1}]$ for some integer n. Because $\mathbf{Z}[n^{-1}]$ is a noetherian ring, $\operatorname{End} M$ is a noetherian module. The submodule $R/\operatorname{Ker}\mu$ is finitely generated over $\mathbf{Z}[n^{-1}]$, and therefore also finitely generated as a ring. By the Structure Theorem,

$$R/\operatorname{Ker}\mu \cong \mathbf{Z}[m_1^{-1}] \times \cdots \times \mathbf{Z}[m_k^{-1}]$$

for some simply composite, positive integers m_j. The module M will split up as a direct sum

$$M = M_1 \oplus \cdots \oplus M_k,$$

with each M_j a torsion-free module over $\mathbf{Z}[m_j^{-1}]$. Because these rings are principal, the modules M_j are in fact free, and we have proved:

Theorem 11. — *Consider a module* M *over a binomial ring. Suppose* M *is torsion-free and finitely generated over* $\mathbf{Z}[n^{-1}]$ *for some integer* n. *There exist positive integers* m_j, r_j *such that*

$$M \cong \mathbf{Z}[m_1^{-1}]^{r_1} \oplus \cdots \oplus \mathbf{Z}[m_k^{-1}]^{r_k}$$

as a module over

$$\mathbf{Z}[m_1^{-1}] \times \cdots \times \mathbf{Z}[m_k^{-1}].$$

References

[1] Burris & Sankappanavar: *A Course in Universal Algebra*, Springer-Verlag 1981.

[2] Torsten Ekedahl: *On minimal models in integral homotopy theory*, Homotopy, Homology and Applications 4, no. 2, part 1, 2002.

[3] Jesse Elliott: *Binomial rings, integer-valued polynomials, and λ-rings*, Journal of Pure and Applied Algebra 207, 2006.

[4] Solomon W. Golomb: *Iterated Binomial Coefficients*, The American Mathematical Monthly, volume 87, no. 9, 1980.

[5] Philip Hall: *The Edmonton Notes on Nilpotent Groups*, Queen Mary College Mathematics Notes 1976.

[6] Jean-Pierre Jouanolou: *Théorèmes de Bertini et Applications*, Birkhäuser 1983.

[7] Clarence Wilkerson: *Lambda-Rings, Binomial Domains, and Vector Bundles over CP*(∞), Communications in Algebra 10 (3), 1982.

[8] Qimh Xantcha: *The Theory of Polynomial Functors*, doctoral dissertation, Stockholm University 2010.

[9] Qimh Richey Xantcha: *Polynomial Maps of Modules*, submitted.

[10] Qimh Richey Xantcha: *Polynomial Functors of Modules*, submitted.

[11] Donald Yau: *Lambda-Rings*, World Scientific 2010.